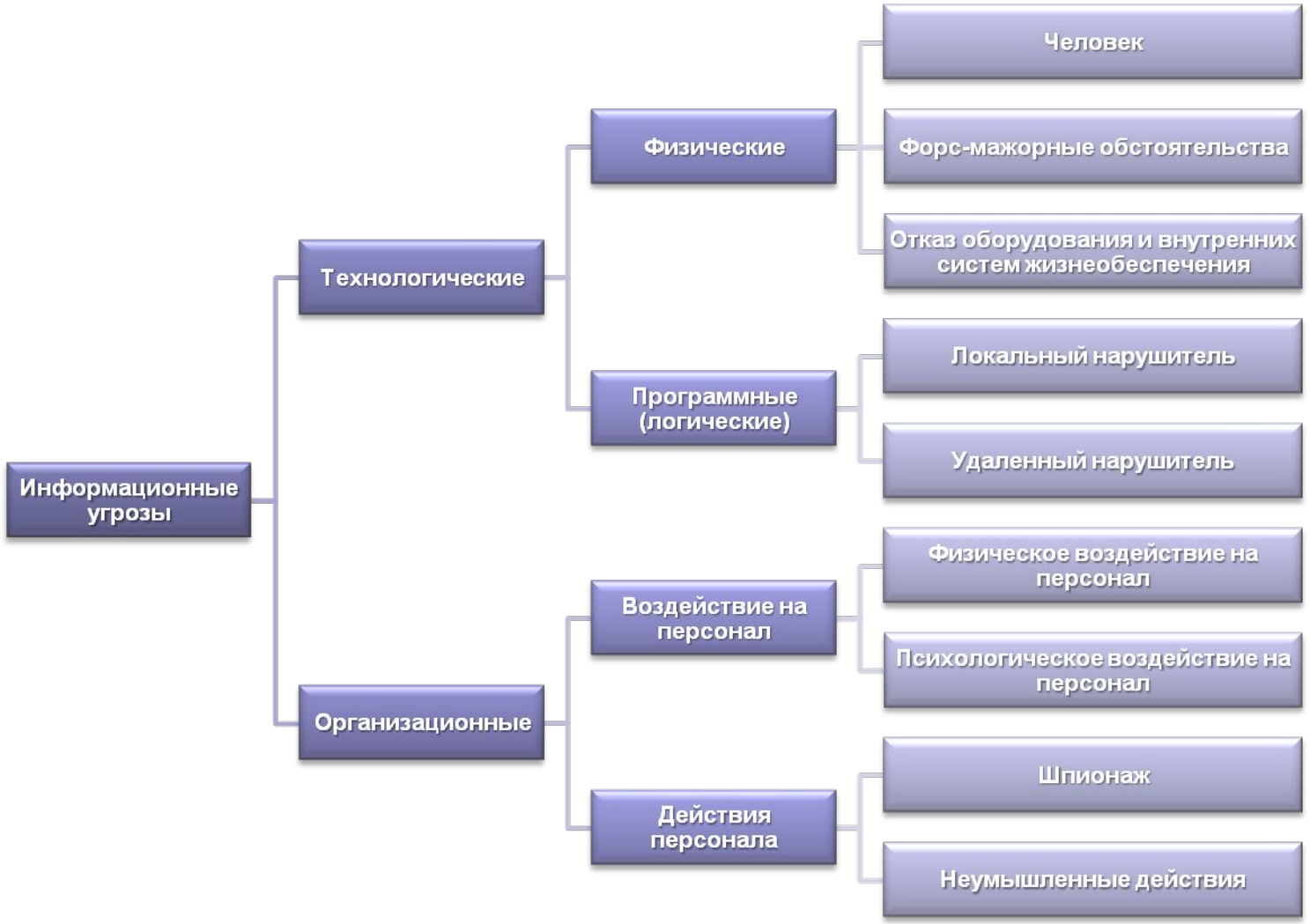
Обеспечение информационной безопасности

Угроза безопасности компьютерной системы - это потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Анализ угроз проведенных агентством национальной ассоциацией информационной безопасности (National Computer Security Association) в США выявил следующую статистику:

Виды информационных угроз



Политика безопасности - это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности.

Организационная защита

- ***организация режима и охраны***.
- ***организация работы с сотрудниками*** (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- ***организация работы с документами*** и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- ***организация использования технических средств*** сбора, обработки, накопления и хранения конфиденциальной информации;
- ***организация работы по анализу внутренних и внешних угроз*** конфиденциальной информации и выработке мер по обеспечению ее защиты;
- ***организация работы по проведению систематического контроля за работой персонала*** с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- Устройства для шифрования информации (криптографические методы).
- Системы бесперебойного питания:
  - Источники бесперебойного питания;
  - Резервирование нагрузки;
  - Генераторы напряжения.

Программные средства защиты информации

- Средства защиты от несанкционированного доступа (НСД):
  - Средства авторизации;
  - Мандатное управление доступом;
  - Избирательное управление доступом;
  - Управление доступом на основе ролей;
  - Журналирование (так же называется Аудит).
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей:
  - Системы обнаружения и предотвращения вторжений (IDS/IPS).
  - Системы предотвращения утечек конфиденциальной информации (DLP-системы).
- Анализаторы протоколов.
- Антивирусные средства.

Программные средства защиты информации

- Межсетевые экраны.
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.
- Системы резервного копирования.
- Системы аутентификации:
  - Пароль;
  - Ключ доступа (физический или электронный);
  - Сертификат;
  - Биометрия.
- Инструментальные средства анализа систем защиты:
  - Мониторинговый программный продукт.

Понятие компьютерного вируса

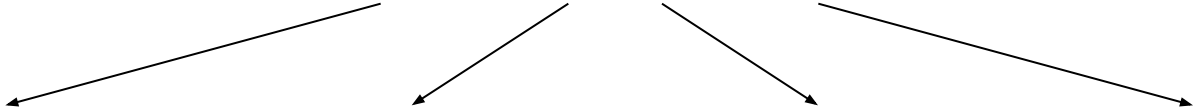
Компьютерный вирус – это специальная программа, наносящая заведомый вред компьютеру, на котором она запускается на выполнение, или другим компьютерам в сети.

Основной функцией вируса является его размножение.

Классификация компьютерных вирусов

- **по среде обитания;**
- **по операционным системам;**
- **по алгоритму работы;**
- **по деструктивным возможностям.**

1) По среде обитания



Файловые вирусы

Наносят вред файлам. Создают файл-двойник с именем оригинала.

Загрузочные вирусы

внедряются в загрузочный сектор диска. Операционная система при этом загружается с ошибками и сбоями

Макро-вирусы

«Портят» документы Word, Excel и других прикладных программ операционной системы Windows.

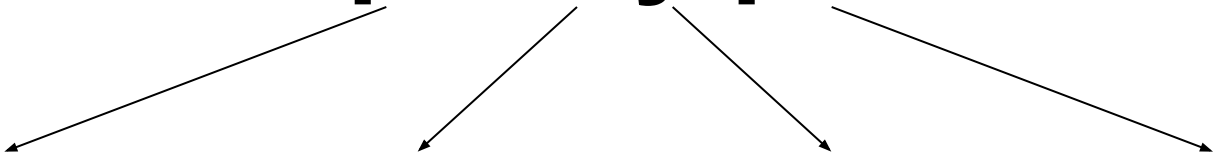
Сетевые вирусы

Распространяются по Internet через электронные письма или после посещения сомнительных сайтов.

2) По операционным системам

Для каждой операционной системы создаются свои вирусы, которые будут «работать» только в ней. Но существуют и универсальные вирусы, которые способны внедряться в различные операционные системы.

3) По алгоритму работы



Резидент-ность

Вирусы, обладающие этим свойством действуют постоянно пока компьютер включен.

Самошифро вание и полимор-физм

Вирусы-полиморфики изменяют свой код или тело прог-раммы, что их трудно обнаружить.

Стелс–алгоритм

Вирусы-невидимки «прячутся» в оперативной памяти и антивирусная программа их не может обнаружить.

Нестан-дартные приемы

Принципиаль но новые методы воздействия вируса на компьютер.

4) По деструктивным возможностям

Безвред-ные
не наносят никакого вреда ни пользовате-лю, ни компьютеру, но занимают место на жестком диске.

Неопасные
наносят моральный ущерб пользователю Вызывают визуальные графические или звуковые эффекты.

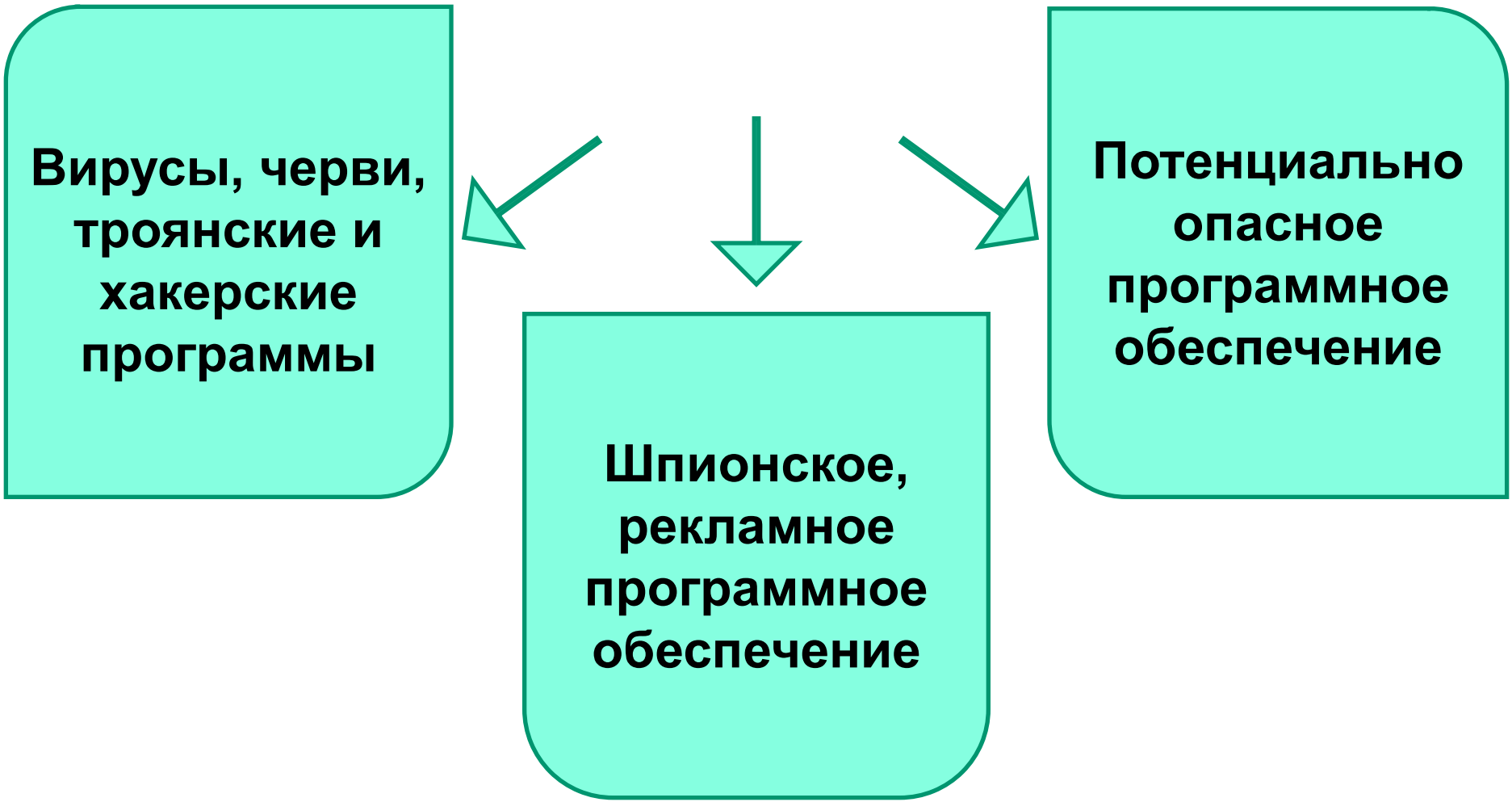
Опасные
уничтожают информацию в файлах. «Портят» файлы, делают их несчитыва-емыми и т.д.

Очень опасные
сбивают процесс загрузки ОС, после чего требуется ее переустановка; или «портят» винчестер, что его требуется форматировать

Защита от вредоносных программ

Вредоносная программа (буквальный перевод англоязычного термина **Malware**, **mal***icious* — злонамеренный и *soft***ware** — программное обеспечение, жаргонное название — «малварь», «маловарь», «мыловарь» и даже «мыловарня») — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.

Вредоносные программы



Антивирусные программы

Современные антивирусные программы обеспечивают ***комплексную защиту программ*** и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер:

- Интернет,
- локальная сеть,
- электронная почта,
- съемные носители информации.

Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусные программы

Для поиска известных вредоносных программ используются сигнатуры. ***Сигнатура*** — это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению или удалению.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т. е. анализа последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

Большинство антивирусных программ сочетает в ***себе функции постоянной защиты*** (антивирусный монитор) и ***функции защиты по требованию пользователя*** (антивирусный сканер).

Антивирусный монитор запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия. Основная задача антивирусного монитора состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольный момент пользователем. Антивирусный сканер производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

Признаки заражения компьютера

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD/DVD дисковода;
- произвольный запуск на компьютере каких-либо программ;
- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- исчезновение или изменение файлов и папок;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- зависание или неожиданное поведение браузера (например, окно программы невозможно закрыть).

Некоторые характерные признаки поражения сетевым вирусом через электронную почту:

- друзья или знакомые говорят о полученных от вас сообщениях, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Действия при наличии признаков заражения компьютера

Прежде чем предпринимать какие-либо действия, необходимо сохранить результаты работы на внешнем носителе (дискете, CD- или DVD-диске, флэш-карте и пр.).

Далее необходимо:

отключить компьютер от локальной сети и Интернета, если он к ним был подключен;

если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;

запустить антивирусную программу.

Компьютерные вирусы и защита от них

Компьютерные вирусы являются вредоносными программами, которые могут «размножаться» (самокопироваться) и скрытно внедрять свои копии в файлы, загрузочные сек

торы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Название ***«вирус»*** по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

По «среде обитания» вирусы можно разделить на загрузочные, файловые и макровирусы.

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса. При инфицировании диска вирус в большинстве случаев переносит оригинальный загрузочный сектор в какой-либо другой сектор диска.

Профилактическая защита от загрузочных вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.

Файловые вирусы

Файловые вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т. е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

Практически все ***загрузочные и файловые вирусы резидентны*** (стирают данные на дисках, изменяют названия и другие атрибуты файлов и т. д.).

Лечение от резидентных вирусов затруднено, так как даже после удаления зараженных файлов с дисков, вирус остается в оперативной памяти и возможно повторное заражение файлов.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительных источников и предварительно не проверенные антивирусными программами.

Макровирусы

Существуют макровирусы для интегрированного офисного приложения Microsoft Office. Макровирусы фактически являются макрокомандами (макросами), на встроенном языке программирования Visual Basic for Applications, которые помещаются в документ.

Макровирусы содержат стандартные макросы, вызываются вместо них и заражают каждый открываемый или сохраняемый документ.

Макровирусы являются ограниченно резидентными.

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Microsoft Office сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе.

Сетевые черви и защита от них

Сетевые черви являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Активизация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

Для своего распространения сетевые черви используют разнообразные сервисы глобальных и локальных компьютерных сетей: Всемирную паутину, электронную почту и т. д.

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — как он передает свою копию на удаленные компьютеры. Однако многие сетевые черви используют более одного способа распространения своих копий по компьютерам локальных и глобальных сетей.

Web-черви

Отдельную категорию составляют ***черви, использующие для своего распространения web-серверы***. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и модифицирует web-страницы сервера. Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают в браузере зараженную web-страницу), и таким образом проникает на другие компьютеры сети.

Разновидностью Web-червей являются ***скрипты*** — активные элементы (программы) на языках JavaScript или VBScript.

Профилактическая защита от web-червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

Еще более эффективны Web-антивирусные программы, которые включают межсетевой экран и модуль проверки скриптов на языках JavaScript или VBScript

Межсетевой экран

Межсетевой экран (брандмауэр) — это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет ее, либо пропускает в компьютер, в зависимости от параметров брандмауэра.

Межсетевой экран обеспечивает проверку всех web-страниц, поступающих на компьютер пользователя. Каждая web-страница перехватывается и анализируется межсетевым экраном на присутствие вредоносного кода.

Распознавание вредоносных программ происходит на основании баз, используемых в работе межсетевого экрана, и с помощью эвристического алгоритма. ***Базы*** содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. ***Эвристический алгоритм*** позволяет обнаруживать новые вирусы, еще не описанные в базах.

Почтовые черви

Почтовые черви для своего распространения используют электронную почту.

Червь либо отсылает свою копию в виде вложения в электронное письмо, либо отсылает ссылку на свой файл, расположенный на каком-либо сетевом ресурсе. В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

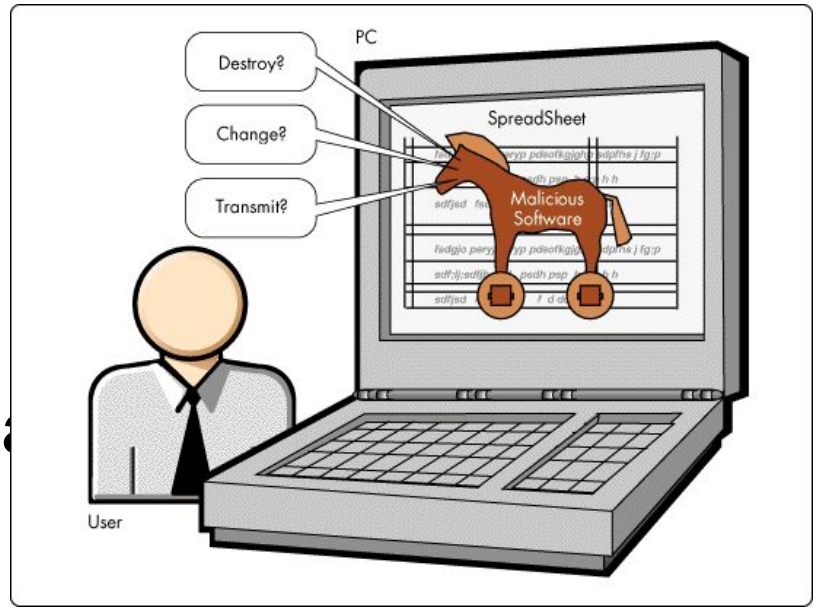
Червь после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя.

Профилактическая защита от почтовых червей состоит в том, что

- не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.
- рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

Троянские программы и защита от них

Троянская программа, троянец (от англ. trojan) — вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.



Троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. Утилиты скрытого управления позволяют принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Являются одним из самых опасных видов вредоносного программного обеспечения.

Троянские программы - шпионы

Троянские программы — шпионы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в каком-либо файле на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Рекламные программы

Рекламные программы (англ. *Adware: Advertisement* — реклама и *Software* — программное обеспечение) встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Рекламные программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять ее злоумышленнику.

Защита от троянских программ. Троянские программы часто изменяют записи системного реестра операционной системы, который содержит все сведения о компьютере и установленном программном обеспечении. Для их удаления необходимо восстановление системного реестра, поэтому компонент, восстанавливающий системный реестр, входит в современные операционные системы.

Хакерские утилиты и защита от них

Сетевые атаки

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них многочисленные запросы. Это приводит к отказу в обслуживании (зависанию сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

Утилиты взлома удалённых компьютеров

Утилиты взлома удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во взломанную систему других вредоносных программ.

Утилиты взлома удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

Руткиты

Руткит (от англ. root kit — «набор для получения прав root») — программа или набор программ для скрытого взятия под контроль взломанной системы.

Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Руткиты модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Защита от хакерских атак, сетевых червей и троянских программ.

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана.

Межсетевой экран позволяет:

- блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);
- не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);
- препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Классификация вирусов по особенностям алгоритма

Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны ***вирусы-невидимки***, называемые ***стелс-вирусами,*** которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Наиболее трудно обнаружить ***вирусы-мутанты***, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые ***квазивирусные*** или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Недостатки антивирусных программ

- Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.
- Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах.
- Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.[8]